http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (5): 814-819, 2008
ISSN 1812-5638


# Distributed IDS in Case of Continuous Attack and Performance Analysis of Access Points

A.K. Kakakhel and N. Anjum
City University of Science and Technology, Peshawar, Pakistan

**Abstract:** The shared nature of wireless network and design of MAC protocol allowed multiple networks to share the same space and radio channel. Intruders could easily inject limitless traffic into the radio network without being attached to wireless access point and could easily lessen the performance level of WLAN as well as access point. We presented a very simple methodology to produce the continuous attack (continuous injection of arbitrary packets into access point) by using Solar winds tool, WAN Killer and monitor the performance of access point using other solar winds tool Network performance monitor. We have taken into consideration different parameters to perform analysis of performance of access point during continuous attack, but the key parameters were average response time and packet lose ratio. Based on this analysis, we proposed some security enhancement features for access point so that the performance level of access point during continuous attack could be raised.

**Key words:** DoS, WLAN, response time, IDS, SNMP

## INTRODUCTION

The shared nature of wireless medium, combined with commodity nature of wireless technologies and an increasing sophisticated user-base, allows wireless networks to be easily monitored and broad cast on. Intruder may easily observe communications between wireless devices and just as easily launch simple denial of services attack against wireless network by injecting false messages (Wenyuan *et al*., 2005). Malicious packets can not be prevented from reaching an access point or client as opposed to wired network.

The MAC protocol is designed to allow multiple networks to share the same space and radio channel. Intruders could easily inject traffic into the radio network without being attached to wireless AP. Intruders wishing to take out the wireless network could send their own network traffic on the same radio channel and the target network would accommodate the new traffic as best it could using the CSMA/CD mechanism in standard. So the reach of wireless network is difficult to control thus allowing the intruder easy physical access. This means that strong security is an absolute for wireless network (Peter, 2006).

In recent years security has become a crucial aspect of wireless technology. Traditional DoS attack could easily be launch with over flowing user domain and kernel domain buffer (Wenyuan *et al*., 2005). The availability of open source code makes it easier for attackers to craft their own WLAN device to mount an attack. Open source projects such as air jack, WAN Killer common view Wi-Fi etc even allow injecting arbitrary frames into a wireless LAN network.

DoS attacks can be roughly classified according to the OSI layering model. Application level DoS attack, DoS at Internet work level, Protocol/Media access level DoS and physical level DoS (radio jamming, interference). As opposed to physical layer attacks it is comparably easy to exploit vulnerabilities in the MAC protocol. The 802.11 MAC is based on the premises of cooperation among all network participants. One of the most prominent DoS attack on WLAN protocol in based on a MAC protocol flaw in 802.11 where, CCA (Clear Channel Assessment) can be used to simulate a busy network to all WLAN clients. A very simple way to thresh the performance of the wireless medium is to constantly cause collision by sending arbitrary data during the legitimate transmission of other clients, this leads to excessive transmission and thus further increasing problem. This collision periods not need be long, in fact a single bit error in the CRC32 protection data section suffices to corrupt a frame, however longer the collision periods are the higher are the chances that there is indeed a collision at the receiver and cause to increase packet loss ratio and decrease network performance. So, it is important for network administrator to constantly monitor the network performance by examining the behavior of Access point (Peter, 2006).

In this study, we propose a very simple methodology for monitoring the performance of access point during continuous attack (continuous injection of arbitrary

**Corresponding Author:** Adil Khan Kakakhel, City University of Science and Technology, Peshawar, Pakistan

packets) and suggest some security enhancement features for access point. We have taken into consideration different parameters to perform analysis of performance of access point during continuous attack but the key parameters, we have discussed are average response time and packet lose ratio. Such system in hand of network administrator can give it a good way to prevent continuous attack and improve performance level of Wi-Fi. The first contribution of this work is to propose a simple methodology to produce the DoS attack at media access level by injecting arbitrary packets to the access point by using Solar Wind's tool WAN Killer (http://www.solarwinds.com).

The proposed procedure includes the small Wi-Fi setup and the software tools for processing results. The main effort was investigated in order to minimize the performance of access point as much as possible. The second contribution of this work is the measurements of results obtained following our proposed methodology from an SNMP protocol enabled D-Link AP using Solar Winds tool, Network Performance monitor. Moreover, the analysis of test results suggests some security enhancement features for AP so, that the continuous attack on Wi-Fi could be prevented.

## RELATED WORK

IDS for cable network have been excessively studied but this is not in case of wireless networks. In wireless network though, many attacks happen at the MAC layer and thus, it is difficult to isolate sequence of packets to use them in such IDSs. Actually, most of work has been done till now refers to Intrusion prevention system (Konstantinos and Iliofotou, 2006).

Wenyuan *et al.* (2005) has presented intrusion detection system at physical layer for radio interference attack. Physical layer jamming is probably the most feasible jamming technique, as it just concern with emitting signal on the shared medium and colliding the communication. They have presented four different jamming attack modal i.e., constant jamming, deceptive jamming, random jamming and reactive jamming that can be use by adversary to disable the operation of wireless network and evaluate their effectiveness in term of how each method effect the ability of a wireless node to send and receive packets. Authors proposed four basic detection schemes signal strength measurement, carrier sensing time, Packet Delivery Ratio (PDR) measurements and location consistency check. Signal strength and carrier sensing time detecting schemes can distinguish the reactive and random Jammer, but it cannot distinguish the reactive and random Jammer. Packet Delivery Ration (PDR) can detect all types of jammers. When there is jamming attack PDR drop to 0. On the other hand there are situations the PDR measurements can lead to false alarms. When there is network failure, like a battery failure, the node in consideration stop sending packets, so, PDR drops to 0 too. So, PDR measurements cannot distinguish between jamming scenario and network failure scenario that can disrupt the communication between the two nodes. On the other hand location consistency check can detect all types of PHY jammers and also distinguish from normal congested networks states or dynamic failures of network though, there are some issues that are critical for their performance, such like the frequency of the location advertisement, which need to be taken into consideration.

Aime *et al.* (2006) have proposed a distributed intrusion detection system in which each node monitor the traffic flow on the network and collects relevant statistics about it, by combining each node's view we are able to tell (and which type of ) an attack happened or if the channel is just saturated. However this system opens the possibility for misuse. No doubt that proposed Intrusion detection system for wireless network based on, distributed collection of relevant information can be helpful in detecting jamming attacks and helps in providing better services to customers by enforcing the operator to have decent services. However, this modal has some drawbacks, which put limits to the performance of wireless networks. In order to work nodes need to exchange their events lists. If a node is being jammed he/she will not be able to exchange data on real time during the attack period but the evidence will be shared in later time. The result is this scheme cannot actually be employed for real time detection. List of events exchange among nodes actually contains very important information about each packet exchange among nodes. For example source address, destination address subtype, FCS, frame number etc. However, these lists of events are exchange in free format i.e., unencrypted. No security mechanism had provided to secure this important information, which opens a free way for attacker to hijack a network and sabotage the performance of entire network without involving extra efforts.

Mika (2000) has given general introduction of radio jamming attack and explore jamming resistance against two popular mobile networks: GSM and WLAN. Author has performed analysis of radio interference of these two networks and calculated effective jamming to noise ratio. Based on the results, author gives some suggestions on how to increase the jamming resistance of network.

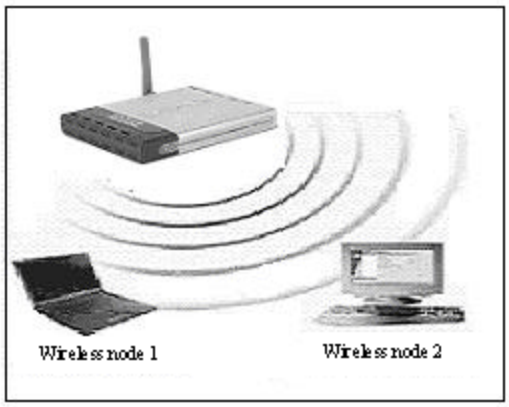


Fig. 1: Wi-Fi Setup for implementing continuous attack

## CONTINUOUS ATTACK

Continuous attack refers to continuous injection of arbitrary packets into wireless medium during legitimate transmission of other clients and thus leads to increasing problems in network such as increase in packet lose ratio, decrease in average response time of access point and increase in corruption rate of frame.

We have implemented continuous attack by setup small W$_i$-F$_i$ environment (Fig. 1) The Wi-Fi setup is comprised of five different nodes each with different function and purpose. i.e., two Wi-Fi cards one access point, one PC with Intel Pentium 3 processor 993 MHZ and 256 MB of RAM and one laptop.

The goal of the tests that we will presents in next section is to produce significant examples of the possible behavior of 802.11 b/g access points during continuous attack. The test procedure is intentionally very simple. However, the behavior of access point coming from these tests is accurate.

We inject arbitrary packets from wireless node 1 with different data rates on access point using WAN Killer tool. The tests were run for 1 h producing a record for each packet received at destination wireless node 2, while on wireless node 2 we were monitoring the performance of access point during continues attack using solar winds tool's Network performance Monitor. Note that all the received packets were included in our analysis, without leaving any warm-up period. During the test and setup of the network used for testing, the operating system Windows XP was used for both wireless node 1 and wireless node 2. There is no particular reason for this choice beside the software tool available to use when testing behavior of access point. The choice of access point was very simple. The access point available for testing purpose was D-Link Air Plus Xtreme G DWL-2100.The access point was configured to use with enabled SNMP protocol to gather traffic statistics of access point during continuous attack i.e., average response time, packet lose ratio and availability of access point during continuous attack. The channel was set to 11 for no special reason and traffic is allowed from both W$_i$-F$_i$ adopters. Two wireless nodes i.e., wireless node 1 and wireless node 2 are the only ones allowed connecting to access point. Most AP have name that the wireless client can use to associate with it and in our test setup the IP address of access point i.e., 192.168.0.50 is used for establishing connection.

WAN Killer was used for running continuous attack on wireless node 1, toward wireless node 2 in the test network and ZD1211 Wi-Fi card was used as 802.11 b/g client interface. WAN Killer was configured using different packet size, circuit bandwidth, percent of bandwidth sliders and port no for injecting traffic towards AP. The detail of configuration of WAN Killer is given in next section. WAN Killer is a tool which can generate random traffic either on wireless or wired network. It sets the circuit bandwidth and the percent of load needed and WAN Killer will generate random traffic.

Network Performance Monitor tool was run on interface of wireless node 2, situated between wireless node 1 and access point, having its NIC D-Link air plus extreme Wi-Fi card set to monitor mode. Solar winds network performance monitor was able to track network latency, packet loss, traffic and bandwidth usage and many other network statistics. The Network Performance Monitor can also monitor each managed node and interface via SNMP protocol to report when a node reboots or an interface goes down. Solar Winds Network performance monitor was used using standard configuration except that, Interface Poll Frequency was set to 90 sec (to update the Interface Details statistics) and Rediscover Interval (to verify and update the identity information) was configured to 30 min and response of AP to SNMP protocol was set to enable.

**Test environment:** Performance of IEEE 802.11 radio data link depends on many environmental factors as fallows:

- Distance between the different radios stations (i.e., radio signal attenuation with propagation)
- Presence of noise or radio channel interference sources
- Physical obstacles like walls, windows, furniture etc.
- Radio signal reflections (radio signal multi-paths and scattering)

All these factors are important contributors to the entire system behavior, In order to obtain the correct results, it is necessary to create the best possible environmental conditions:

- No 802.11 radio channel interferences
- Short distance between the different wireless nodes (but higher than the minimum recommended one)
- A small environment to minimize radio multi-paths effects

To achieve the correct results we recommended the experiments in an environment with no other active access point, except the one under test. All the wireless nodes used for the test have to be placed in a single small room, such as office or class room. Non 802.11 radio devices may interfere with access point under test. For example: microwave ovens, cordless phones etc. Therefore, we make sure the absences of such devices. Our test environment recommendations aim to provide a general framework to select a proper location for measuring the AP's behaviors during continuous attack.

## ACCESS POINT PERFORMANCE

In order to test the performance level of access point during continuous attack, several tests were conducted to gain as much information as possible regarding the network in question. Firstly nodes needs to connect to AP in order to access to network. Secondly once nodes have connected to the AP both need to be configure in order to execute continuous attack and gather statistics of AP performance.

This section presents the results of the tests we performed on D-Link 2100 AP models according to our procedure and it has two aims:

- The first one is to validate our recommended test procedure
- The second one is to verify the general conclusions which we will present in the next section

During the testing and monitoring of traffic between the wireless node 2 and AP, traffic had to be generated via wireless node 1 using Solar Winds tool's WAN Killer.Wan Killer was configured using different data rates to offered as much as load to AP as possible. But we are describing here only three tests we performed. Table 1 shows the configuration detail of three tests.

We configure the port of WAN Killer to 9-discarded udp to send random traffic towards access point. It discards all traffic when the target device receives and doesn't send back to Wan Killer. This will generate a load in one direction. Wan Killer will always attempt to send the percent of circuit bandwidth set on the slider. Setting the packet size higher will generate the fewer packets, setting a smaller packet size will generate more packets. We configure the percent of bandwidth slider to adjust the amount of data to send to AP and WAN Killer will attempt to generate enough random packets equal to percentage of bandwidth. We have configured the percent of bandwidth slider to maximum of 150% in order to offer load to AP as much as possible. Wan Killer may take 30 sec or more to adjust itself to Windows operating system, IP stack and network.

In order to get correct results, it is necessary to verify the 100% availability of AP during attack. The Network Performance Monitor tool produces this verification. The Fig. 2-4 shows the 100% availability of AP during continuous attack.

Table 1: Configuration detail of Wan Killer for test 1, 2 and 3

| Configuration of WAN killer | Test 1 | Test 2 | Test 3 |
|---|---|---|---|
| Port | 9-discard udp | 9-discard udp | 9-discard udp |
| Packet size | 500 | 1000 | 1500 |
| Circuit bandwidth (Kbps) | 56000 | 56000 | 56000 |
| Bandwidth slider (%) | 100 | 110 | 150 |

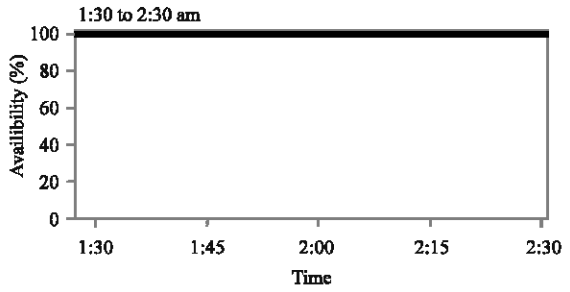


Fig. 2: Availability of AP during test 1

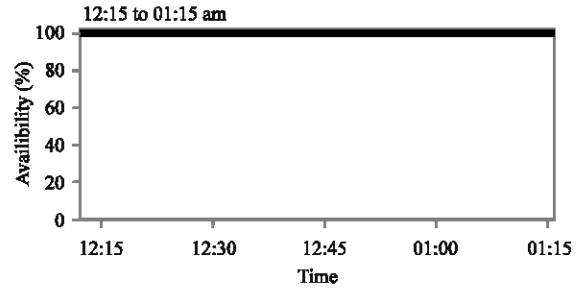


Fig. 3: Availability of AP during test 2

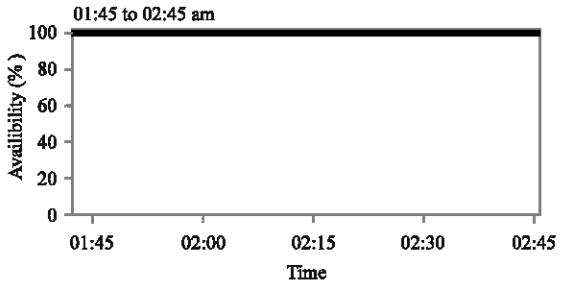


Fig. 4: Availability of AP during test 3

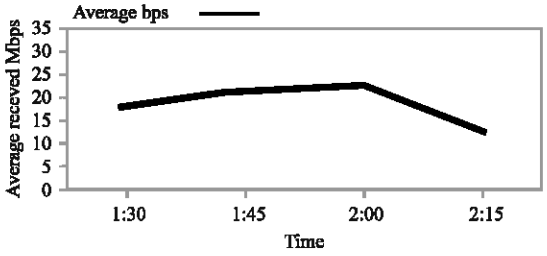


Fig. 5: Average receive bps by AP during test 1

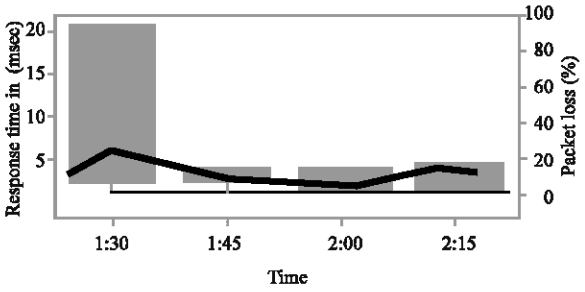


Fig. 6: Average response time and packet lose ratio during test 1

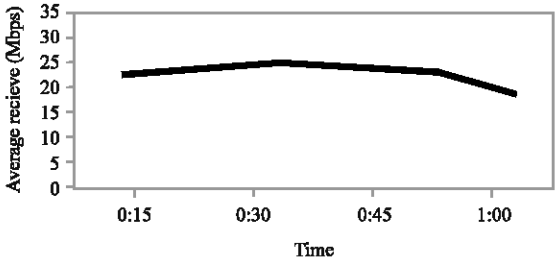


Fig. 7: Average receive bps by AP-Recv bandwidth 54 Mbps during test 2

For maximum offered load between 18 to 23 Mbps (Fig. 5) to AP during test 1 the average response time of AP decrease from 0 to 6 msec (Fig. 6).

For maximum offered load between 23 to 25 Mbps (Fig. 7) to AP during test 2 the average response time of AP decrease from 0 to 220 msec (Fig. 8).

But packet lose ratio for both of offered load to AP remains 0%. Instead for both offered load to AP Network Performance Monitor shows significant decrease in response time but it requires further investigation. We injected maximum packets to AP via wireless node 1 to wireless node 2 during test 3. For maximum offered load between 25 to 29 Mbps (Fig. 9) to AP we get unexpected results.

As compared to previous two results we observe that AP couldn't bridge all incoming packets, therefore, it starts dropping packets and its packet lose ratio decrease up to 30% and average response time decrease up to

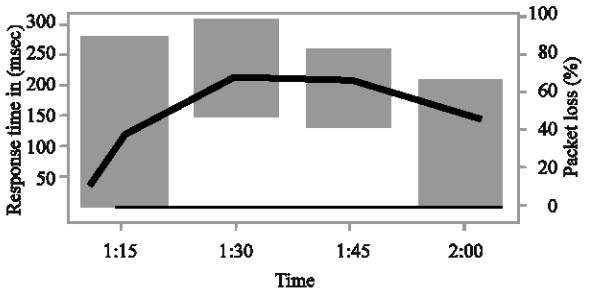


Fig. 8: Average response time and packet lose ratio during test 2

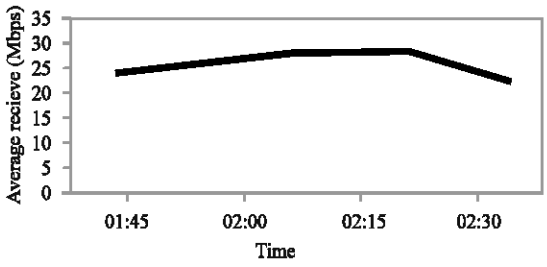


Fig. 9: Average receive bps by AP during test 3

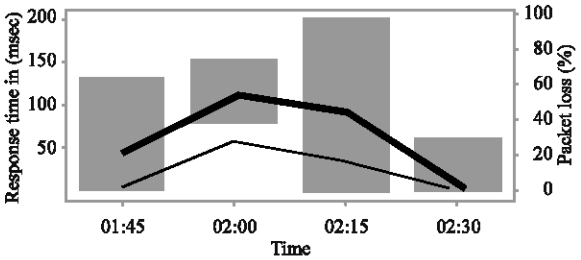


Fig. 10: Average response time and packet lose ratio during test 3

120 msec (Fig. 10) which was very lessen than previous results. The fact is AP can handle maximum of 25 Mbps traffic. More traffic put significant impact on the performance level of AP.

## CONCLUSION AND FUTURE WORK

In this study, we present a very simple methodology to implement continuous attack on wireless network and monitor the performance of AP during attack using Solar Winds tool, network performance monitor using parameters response time and packet lose ratio by AP.

From the attack described and results shows that, attacker can easily launch continuous attack using different and high data rates which not only cause to decrease average response time of AP as it has been

shown in test 1, 2 and 3 but also cause to increase packet lose ratio as it has been shown in test 3 in which packet lose ratio of AP was moved up to 30% when packet with large size were injected toward AP. Protection against continuous attack is very difficult due to free availability of attacker tools but by implementing following security enhancement features in AP continuous attack can be prevented:

- AP must be designed as SNMP enabled device which will help network administrators to obtain a great amount of data regarding the status of the device and its functioning
- Some type of Methods and systems of dynamic channel allocation for every access points should be adopted. Since continuous attacks are implemented by injecting arbitrary packets continuously towards fixed channels on which AP is listening therefore, in case of continuous attacks, should be able to change the channel dynamically. Thus, a method for dynamic channel allocation for access points in wireless networks is desirable
- Attack channel should be blocked in response of the attack
- Some sort of ping utility is desirable in AP's to inform administrator about attack
- The information collected by administrator must be sent to trusted clients as to facilitate distributed IDS

Although, in this study, we have studied continuous attack on Wi-Fi using only one access point but for future work we will consider other available access points and discuss and compare their performance level during continuous and other DoS level attacks and will explore weaknesses in AP's. Also, we would like to come up with some sort of efficient algorithm for distributing the attacker's information between trusted clients.

## ACKNOWLEDGMENTS

I would like to thank my Supervisor Mr. Adil Kakakhel from City University of science and technology Peshawar, Pakistan for his advice and feedback on the ideas expressed in this research. I would also like to thank Head of Dept. Mr. Abdus Salam for giving us opportunity for sharing our work and vision in the area of $W_i$-$F_i$ of University.

## REFERENCES

Aime, M.D., G. Calandriello and A. Lioy, 2006. A wireless distributed intrusion detection system and a new attack model. Proceedings of 11th Symposium on Computers and Communications, ISCC 06. September 11, IEEE, pp: 35-40.

Konstantinos, P. and M. Iliofotou, 2006. Denial of service attacks in wireless networks: The case of Jammer, 2006. Department of Computer Science and Engineering UC Riverside, Riverside CA 92521. http://www.cs.ucr.edu/~kpele/Jamming.pdf.

Mika, S., 2000. Radio jamming attacks against two popular mobile networks. Helsinki University of Technology, HUT TML 2000, Tik-110-501 Seminar on Network security fall 2000 http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/stahlberg.pdf.

Peter, E., 2006. Susceptibility of wireless devices to denial of service attacks. White Paper Embedded World 2006, Net Module Meriedweg 11,CH-3172 Niederwangen, Switzerland, www.netmodule.com, http://www.netmodule.com/store/publications/susceptibility_of_wireless_devices_to_DoS.pdf.

Wenyuan, X., W. Trappe, Y. Zhang and T. Wood, 2005. The feasibility of launching and detecting jamming attacks in wireless networks. Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing. May 25-27, ACM New York, NY, USA, pp: 46-57.